IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Paul S. Germscheid et al.

Serial No.: N/A Examiner: Unknown

Filing Date: Herewith Group Art Unit: Unknown

For: METHOD AND APPARATUS FOR A WEB APPLICATION SERVER TO PROVIDE FOR WEB USER VALIDATION

Docket No.: 33012/274/101

TRANSMITTAL SHEET

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

CERTIFICATE UNDER 37 C.F.R. 1.10: The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, "Express Mail Post Office to Addressee" having an Express Mail mailing label number of : EL 522 531 619 US, in an envelope address to: Assistant Commissioner for Patents, Washington, D.C., 20231 on this 24th day of November, 1999.

By John L. Rooney
John L. Rooney

We are transmitting herewith the attached Patent Application including the following:

[XXXX] 40 sheet(s) of specification.

[XXXX] 4 sheet(s) of claim(s).

[XXXX] 1 sheet(s) of Abstract.

[XXXX] 14 sheet(s) of drawings.

[XXXX] Executed Declaration and Power of Attorney.

[ ] A verified statement(s) to establish small entity status under 37 C.F.R. 1.9 and/or 1.27 is enclosed.

[XXXX] An Assignment of the invention to Unisys Corporation is being filed contemporaneous with this patent application.

[ ] A certified copy of a _____ application, serial no. _____, filed _____, 19___, the right of priority of which is claimed under 35 U.S.C. 119.

CLAIMS AS FILED						
	(1)	(2)	SMALL ENTITY		OTHER	
FOR:	# FILED	# EXTRA	Rate	Fee	Rate	Fee
BASIC FEE				$380		$760
TOTAL CLAIMS	20-20 =	0	x9=	$	x18=	$ 0
INDEPENDENT CLAIMS	4 -3 =	1	x39=	$	x78=	$ 78
( ) MULTIPLE DEPENDENT CLAIM PRESENTED			+130=	$	+260=	$ 0
TOTAL			$		$838.00	

*If the difference in Column (1) is less than zero, enter "0" in Column 2.

[XXXX] Other Recordation Form Cover Sheet-Patents Only.

[XXXX] Checks in the amounts of $838.00 and $40.00 are enclosed.

[XXXX] Please charge any deficiencies or credit any overpayment in the enclosed fees to Deposit Account 14-0620.

By: John L. Rooney

John L. Rooney
Reg. No. 28,898

NAWROCKI, ROONEY & SIVERTSON, P.A.
Suite 401, Broadway Place East
3433 Broadway Street N.E.
Minneapolis, Minnesota 55413
Telephone: (612) 331-1464
Facsimile: (612) 331-2239

METHOD AND APPARATUS FOR A WEB APPLICATION SERVER TO PROVIDE FOR WEB USER VALIDATION

CROSS REFERENCE TO CO-PENDING APPLICATIONS

U.S. Patent Application No. _____, filed _____, and entitled, "A Common Gateway Which Allows Applets to Make Program Calls to OLTP Applications Executing on an Enterprise Server"; U.S. Patent Application No. _____, filed _____, and entitled, "A Multi-Client User Customized DOM Gateway for an OLTP Enterprise Server Application"; U.S. Patent Application No. _____, filed _____, and entitled, "An Automated Development System for Developing Applications that Interface with Both Distributed Component Object Model (DOM) and Enterprise Server Environments"; U.S. Patent Application No. _____, filed _____, and entitled, "Providing a Modular Gateway Architecture Which Isolates Attributes of the Client and Server Systems into Independent Components"; U.S. Patent Application No. _____, filed _____, and entitled, "Making CGI Variables and Cookie Information Available to an OLTP System"; U.S. Patent Application No. _____, filed _____, and entitled, "A Gateway for Dynamically Providing Web Site Status Information"; U.S. Patent Application No. _____, filed _____, and entitled, "Development System for Automatically Enabling a Server Application to Execute with an XATMI-complaint transaction MGR :Managing Transactions within Multiple Environments"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Batch Interface"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Debug"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Workstation Directory/File

Browser"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Icons"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Repository"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Service Templates"; U.S. Patent Application No. _____, filed _____, and entitled, "Automatic Footer Text on HTML Pages"; U.S. Patent Application No. _____, filed _____, and entitled, "Availability Message"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE System Settings"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Service Handler"; U.S. Patent Application No. _____, filed _____, and entitled, "Server Side Variables""; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE data Wizard"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Table Profiling"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Database Profiling";U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Column Profiling";U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Method and Apparatus for a Web Application Server to Maintain Logon Security Mapped to a Gateway Through Server Based Session Objects"; U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE Method and Apparatus for a Web Application Server to Upload Multiple Files and Invoke a Script to Use the Files in a Single Browser Request";U.S. Patent Application No. _____, filed ___ __, and entitled, "Cool ICE Method and Apparatus for a Web Application Server to Provide an Administration System Using a Dual Set of Tiered Groups of Objects"; and U.S. Patent Application No. _____, filed _____, and entitled, "Cool ICE State Management" are commonly assigned co-pending applications incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. **Field of the Invention:** The present invention generally relates to data base management systems and more particularly relates to enhancements for providing secure access to data base management systems via internet user terminals.

2. **Description of the prior art:** Data base management systems are well known in the data processing art. Such commercial systems have been in general use for more than 20 years. One of the most successful data base management systems is available from Unisys Corporation and is called the MAPPER® data base management system. The MAPPER system can be reviewed using the MAPPER User's Guide, incorporated herein by reference, which may be obtained from Unisys Corporation.

The MAPPER system, which runs on various hardware platforms also available from Unisys Corporation, provides a way for clients to partition data bases into structures called cabinets, drawers, and reports, as a way to offer a more tangible format. The MAPPER data base manager utilizes various predefined high-level instructions whereby the data base user may manipulate the data base to generate human-readable data presentations. The user is permitted to prepare lists of the various predefined high-level instructions into data base manager programs called "MAPPER Runs". Thus, users of the MAPPER system may create, modify, and add to a given data base and also generate periodic and aperiodic updated reports using various MAPPER Runs.

However, with the MAPPER system, as well as with similar proprietary data base management systems, the user must interface with the data base using a terminal coupled directly

to the proprietary system and must access and manipulate the data using the MAPPER command language of MAPPER. Ordinarily, that means that the user must either be co-located with the hardware which hosts the data base management system or must be coupled to that hardware through dedicated data links. Furthermore, the user usually needs to be schooled in the command language of MAPPER (or other proprietary data base management system) to be capable of generating MAPPER Runs.

Since the advent of large scale, dedicated, proprietary data base management systems, the internet or world wide web has come into being. Unlike closed proprietary data base management systems, the internet has become a world wide bulletin board, permitting all to achieve nearly equal access using a wide variety of hardware, software, and communication protocols. Even though some standardization has developed, one of the important characteristics of the world wide web is its ability to constantly accept new and emerging techniques within a global framework. Many current users of the internet have utilized several generations of hardware and software from a wide variety of suppliers from all over the world. It is not uncommon for current day young children to have ready access to the world wide web and to have substantial experience in data access using the internet.

Thus, the major advantage of the internet is its universality. Nearly anyone, anywhere can become a user. That means that virtually all persons are potentially internet users without the need for specialized training and/or proprietary hardware and software. One can readily see that providing access to a proprietary data base management system, such as MAPPER, through the internet would yield an extremely inexpensive and universally available means for accessing the data which it contains and such access would be without the need for considerable specialized

training.

There are two basic problems with permitting internet access to a proprietary data base. The first is a matter of security. Because the internet is basically a means to publish information, great care must be taken to avoid intentional or inadvertent access to certain data by unauthorized internet users. In practice this is substantially complicated by the need to provide various levels of authorization to internet users to take full advantage of the technique. For example, one might have a first level involving no special security features available to any internet user. A second level might be for specific customers, whereas a third level might be authorized only for employees. One or more fourth levels of security might be available for officers or others having specialized data access needs.

Existing data base managers have security systems, of course. However, because of the physical security with a proprietary system, a certain degree of security is inherent in the limited access. On the other hand, access via the internet is virtually unlimited which makes the security issue much more acute.

Current day security systems involving the world wide web involve the presentation of a user-id and password. Typically, this user-id and password either provides access or denies access in a binary fashion. To offer multiple levels of secure access using these techniques would be extraordinarily expensive and require the duplication of entire databases and or substantial portions thereof. In general, the advantages of utilizing the world wide web in this fashion to access a proprietary data base are directly dependent upon the accuracy and precision of the security system involved.

The second major problem is imposed by the internet protocol itself. One of the

characteristics of the internet which makes it so universal is that any single transaction in HTML language combines a single transfer (or request) from a user coupled with a single response from the internet server. In general, there is no means for linking multiple transfers (or requests) and multiple responses. In this manner, the internet utilizes a transaction model which may be referred to as "stateless". This limitation ensures that the internet, its users, and its servers remain sufficiently independent during operation that no one entity or group of entities can unduly delay or "hang-up" the communications system or any of its major components. Each transmissions results in a termination of the transaction. Thus, there is no general purpose means to link data from one internet transaction to another, even though in certain specialized applications limited amounts of data may be coupled using "cookies" or via attaching data to a specific HTML screen.

However, some of the most powerful data base management functions or services of necessity rely on coupling data from one transaction to another in dialog fashion. In fact this linking is of the essence of MAPPER Runs which assume change of state from one command language statement to the next. True statelessness from a first MAPPER command to the next or subsequent MAPPER command would preclude much of the power of MAPPER (or any other modern data base management system) as a data base management tool and would eliminate data base management as we now know it.

The practical security problem is to provide individualized access to secure portions of a data base wherein the user employs dialog accessing techniques. In the past, the logic for regulating such secure access was lodged within the logic to honor the service request. This results in duplication of effort and non-compatibility over a range of service request types.

SUMMARY OF THE INVENTION

The present invention overcomes the disadvantages of the prior art by providing a method of and apparatus for utilizing the power of a full featured data base management system by a user at a world wide web browser coupled to the world wide web or internet while maintaining security. Security has typically involved either the encryption of sign on information, or else the using of secure connections requiring more administrative setup. To make access to a proprietary data base by internet users practical, a sophisticated security system is required to prevent intentional or inadvertent unauthorized access to the sensitive data of an organization. In order to permit any such access, the present invention has a security feature that requires a user to sign on with a UserID and Password when secured services are requested. This invention will provide a new SignOn capability which allows for site-specific data to be used to identify a user. The site-specific data is converted to a valid UserID/Password by a User Validation service implemented by a site. This feature requires a site to implement a site-user. The site must also implement a User Validation service. This service will return data in a pre-defined format so that it can be processed.

This unique User Validation feature provides the capability for the browser to send information, which is then translated into a UserID/Password on the Cool ICE Web Application server. This bypasses the need to send a UserID/Password from browser to server, which enhances security.

As discussed above, such a security system should provide multiple levels of access to accommodate a variety of authorized user categories. Site specific profiles may offer only limited

or no access to sensitive data when the user terminal site is not particularly secure. These features can be effectively combined with physical security procedures to provide many specialized security profiles. Each individual service within an ASP may be validated. Other solutions must still transmit sign on over the network for each service. Even though such transmissions may be encrypted or sent over a secure connection, they can still be susceptible to being accessed and decrypted by malicious users. The present approach enhances granularity of security. The UserValidation service is used to convert site specific user validation data to a UserID and Password.

From the system perspective, rather than defining several levels of data classification, the different classes of users and user sites are managed by identifying a security profile as a portion of those service requests requiring access to secure data. Thus, the security profile accompanies the data/service to be accessed. The user simply need execute the sign on procedure which correlates to the access permitted. This permits certain levels of data to be accessed by one or more of the several classes of user.

In the preferred mode of practicing the present invention, a user signs on to the gateway with a generic login protocol providing access as an unsecured user. All users of the gateway sign on in a similar fashion. Should the user request access to a secure function or to secure data, the user validation, rather than the secure service, manages the security profiling technique. The service request for secure access results in the user validation requesting such additional logon information as is required to permit the desired access. In this way, the web browser request is associated with security attributes so that each web user transaction attaches to the database management system object using the security obtained from the Cool ICE session object.

The present invention adds a Access restriction. That is, web applications may be written to require a secured sign on in order to access particular service. A UserID and Password is required to access the service in order to identify a user with the proper security. Often times his UserID and Password is associated with a database that can allow access to sensitive information beyond what the web application server is accessing.

Typically this UserID and Password is entered in a web browser page, and transmitted across the network to the application server which then uses this sign on information to access the service. This may cause a security breach, as network packets may be intercepted, and the sign on information compromised. The invention enhances security in that sign on information is only processed at the application server, and no sign on information is transmitted over a network.

The transaction data in HTML format received by the server from the user, along with the state information stored in the repository, are processed by a service handler into a sequence of service requests in the command language of the data base management system.

Through the use of the repository to store the state of the service request sequence, the service handler to execute data base management commands , the world wide web user is capable of performing each and every data base management function available to any user. In addition, the data base management system user at the world wide web terminal is able to accomplish this without extensive training concerning the command language of the data base management system.

BRIEF DESCRIPTION OF THE DRAWINGS

Other objects of the present invention and many of the attendant advantages of the present invention will be readily appreciated as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, in which like reference numerals designate like parts throughout the figures thereof and wherein:

FIG. 1 is pictographic view of the Cool ICE system coupled between a user on the world wide web and an existing proprietary data base management system;

Fig. 2 is a schematic drawing showing the operation of a multi-level security system in accordance with the preferred embodiment of the present invention;

Fig. 3 is a pictographic view of the hardware of the preferred embodiment;

Fig. 4 is a semi-schematic diagram of the operation of the Cool ICE system;

Fig. 5 is an overall schematic view of the software of the Cool ICE system;

Fig. 6 is a schematic view of a service request;

Fig. 7 shows a schematic view of a service request sequence;

Fig. 8 is a diagrammatic comparison between a dialog-based structure and a service-based structure;

Fig. 9 is a detailed diagram of the storage and utilization of state information within the repository;

Fig. 10 is a detailed diagram showing security profile verification during a service request;

Fig. 11 is a view of the initial Cool ICE Administration window;

Fig. 12 is a view of the security maintenance main window;

Fig. 13 is a diagram showing the creation of a site security profile; and

Fig. 14 is a listing of the messages utilized in creating the site security profile.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is described in accordance with several preferred embodiments which are to be viewed as illustrative without being limiting. These several preferred embodiments are based upon the MAPPER data base management system, and the Cool ICE software components, all available from Unisys Corporation.

Fig. 1 is an overall pictographic representation of a system 10 permitting access to a proprietary data base management system via an internet terminal. Existing data bases and applications 12 represents commercially available hardware and software systems which typically provide select users with access to proprietary data and data base management functions. In the preferred embodiment, existing data bases and applications 12 represents one or more data bases prepared using MAPPER data base management system, all available from Unisys Corporation. Historically, existing data bases and applications 12 could only be accessed from a dedicated, direct terminal link, either physically co-located with the other system elements or connected thereto via a secured dedicated link.

With the preferred mode of the present invention, communication between new web application terminal 14 and existing data bases and applications 12 is facilitated. As discussed above, this permits nearly universal access by users world wide without specialized hardware and/or user training. The user effects the access using standardized HTML transaction language through world wide web link 16 to the Cool ICE system 20, which serves as a world wide web server to world wide web link 16.

Cool ICE system 20 appears to existing data bases and applications 12 as a data base management system proprietary user terminal over dedicated link 18. Oftentimes, dedicated link 18 is an intranet or other localized link. Cool ICE system 20 is currently available in commercial form without the present invention as Cool ICE Revision Level 1.1 from Unisys Corporation.

Fig. 2 is a basic schematic diagram of security system 22 of the preferred mode of the present invention. By way of example, there are four categories of service defined, each with its own functionality and portion of the data base. Service A 36 contains data and functions which should only be made available to customers. Service B 38 contains data and functions which should only be made available to customers or employees. Service C 40 contains data and functions which should only be made available to employees, and Service D 42, containing the least restrictive data and functions may be made available to anyone, including the general public.

In a typical application, Service D 42 might contain the general home page information of the enterprise. It will consist of only the most public of information. It is likely to include the name, address, e-mail address, and phone number of the enterprise, along with the most public of the business details. Usually, Service D 42 would include means of presenting the information in a sufficiently interesting way to entice the most casual of the public user to make further inquiry and thus become more involved with the objectives of the enterprise. Service D 42 represents the lowest level of security with data and functions available to all.

Service C 40 is potentially the highest level of classification. It contains data and functions which can be made available only to employees. In actual practice, this might entail a number of sub levels corresponding to the various levels of authority of the various employees. However, some services may be so sensitive that the enterprise decides not to provide any access via the internet. This might include such things as strategic planning data and tools, advanced financial predictions, specific information regarding individual employees, marketing plans, etc. The penalty for this extreme security measure is that even authorized individuals are prohibited from

accessing these services via the internet, and they must take the trouble to achieve access via an old-fashioned dedicated link.

Customers and employees may share access to Service B 38. Nevertheless, these data and functions are sufficiently sensitive that they are not made public. Service B 38 likely provides access to product specifications, delivery schedules and quantities, and pricing.

For customer access only is Service A 36. One would expect marketing information, along with specific account information, to be available here.

These four service levels (i.e., Service A 36, Service B 38, Service C 40, and Service D 42) are regulated in accordance with three security profiles. The lowest level of security does not require a security profile, because any member of the general public may be granted access. This can be readily seen as guest category 28 (e.g., a member of the public) can directly access Service D 42. Of course, all other categories of user may also directly access Service D 42, because all members of the more restrictive categories (e.g., customers and employees) are also members of the general public (i.e., the least restrictive category).

Security Profile #1, 30 permits access to Service A 36 if and only if the requestor seeking access is a customer and therefore a member of customer category 24. Members of customer category 24 need to identify themselves with a customer identification code in order to gain access. The assigning and processing of such identification codes are well known to those of skill in the art.

Similarly, Security Profile #3, 34 permits access to Service C 40 if and only if the requestor seeking access is an employee and therefore a member of employee category 26. Security Profile #2, 32 permits access to Service B 38 to requestors from either customer

category 24 or employee category 26, upon receipt of a customer identification code or an employee identification code. A more detailed description of the security system of the preferred mode of the present invention is found below.

Fig. 3 is a pictorial diagram of hardware suite 44 of the preferred embodiment of the present invention. The client interfaces with the system via internet terminal 46. Terminal 46 is an industry compatible, personalized computer having a suitable web browser, all being readily available commercial products. Internet terminal 46 communicates over world wide web access 48 using standardized HTML protocol.

The Cool ICE system is resident in web server 50, which is coupled to internet terminal 46 via world wide web access 48. In the preferred mode, web server 50 is owned and operated by the enterprise owning and controlling the proprietary data base management system. Web server 50 may serve as the internet access provider for internet terminal 46. Web server 50 may be a remote server site on the internet if the shown client has a different internet access provider. This would ordinarily occur if the shown client were a customer or guest.

In addition to being coupled to world wide web access 48, web server 50, containing the Cool ICE system, can be coupled to network 52 of the enterprise as shown. Network 52 provides the system with communication for additional enterprise business purposes. Thus, the Cool ICE application on web server 50 and others granted access may communicate via network 52 within the physical security provided by the enterprise. Also coupled to network 52 is departmental server 58 having departmental server storage facility 60. Additional departmental servers (not shown) may be coupled to network 52. The enterprise data and enterprise data base management service functionality typically resides within enterprise server 54, departmental server 58, and any other departmental servers (not shown). Normal operation in accordance with the prior art would provide access to this data and data base management functionality via network

52 to users directly coupled to network 52.

In the preferred mode of the present invention, access to this data and data base management functionality is also provided to users (e.g., internet terminal 46) not directly coupled to network 52, but indirectly coupled to network 52 via web server 50 and the Cool ICE server application components. As explained below in more detail, web server 50 provides this access utilizing the Cool ICE system resident in web server 50.

Fig. 4 is pictographic view of the system of Fig. 3 with particular detail showing the organization and operation of the Cool ICE system 62, which is resident in the web server (see also Fig. 3). In this view, the client accesses the data base management system within the enterprise via internet terminal 54 which is coupled to the web server 68 by world wide web path 66. Again, the internet terminal 54 is preferably an industry standard computer utilizing a commercially available web browser.

The basic request/response format of the Cool ICE system involves a "service" (defined in greater detail below) which is an object of the Cool ICE system. The service is a predefined operation or related sequence of operations which provide the client with a desired static or dynamic result. The services are categorized by the language in which they were developed. Whereas all services are developed with client-side scripting which is compatible with internet terminal 54 (e.g., HTML), the server-side scripting defines the service category. Native services utilize Cool ICE script for all server-side scripting. On the other hand, open services may have server-side scripting in a variety of common commercial languages including Jscript, VBScript, ActiveX controls, and HTML. Because native services are developed in the Cool ICE script (run) language, greater development flexibility and variety are available with this technique.

Web server 68 provides processor 70 for Active Server Pages (ASP's) which have been developed as open services 72 and a Default ASP 73 for invoking native services. After the appropriate decoding within a native or open service, a call to the necessary Cool ICE object 74 is initiated as shown. The selected service is processed by the Cool ICE engine 76.

Repository 80 is a storage resource for long term storage of the Cool ICE service scripts

and short term storage of the state of a particular service. Further details concerning repository 80 may be found by consulting the above referenced, commonly-assigned, co-pending U.S. Patent Application. In the preferred mode of the present invention, the service scripts stored in repository 80 are typically very similar to mapper runs as described above. For a more detailed description of MAPPER runs, MAPPER User Manual is available from Unisys Corporation and incorporated herein by reference.

Cool ICE engine 76 sequences these previously stored command statements and can use them to communicate via network 84 with other data base management system(s) (e.g., MAPPER) resident on enterprise server 86 and/or departmental server 88. The storage capability of repository 80 is utilized by Cool ICE engine 76 to store the state and intermediate products of each service until the processing sequence has been completed. Following completion, Cool ICE engine 76 retrieves the intermediate products from repository 80 and formats the output response to the client, which is transferred to internet terminal 54 via web server 68 and world wide web path 66.

Cool ICE Administrator 82 is available for coordination of the operation of Cool ICE system 62 and thus can resolve conflicts, set run-time priorities, deal with security issues, and serve as a developmental resource. Graphing engine 78 is available to efficiently provide graphical representations of data to be a part of the response of a service. This tends to be a particularly useful utility, because many of the existing data base management systems have relatively sparse resources for graphical presentation of data.

The combination of Cool ICE object 74, Cool ICE engine 76, and repository 80 permits a rather simplistic service request from internet terminal 54 in dialog format to initiate a rather

complex series of data base management system functions. In doing so, Cool ICE engine 76 emulates an intranet user of the data base management system(s) resident on enterprise server 86 and/or departmental server 88. This emulation is only made possible, because repository 80 stores sequences of command language statements (i.e., the logic of the service request) and intermediate products (i.e., the state of the service request). It is these functions which are not available in ordinary dialog on the world wide web and are therefore not even defined in that environment.

Fig. 5 is a schematic diagram 90 of the software components of the Cool ICE system and the software components to which it interfaces in the preferred mode of the present invention. The client user of the Cool ICE system interfaces directly with web browser 92 which is resident on internet terminal 54 (see also Fig. 4). Web browser 92 is a commercially available browser. The only special requirement of web browser 92 is that it be capable of supporting frames.

Web browser 92 communicates with web server software 96 via internet standard protocol using HTML language using world wide web path 94. Web server software 96 is also commercially available software, which is, of course, appropriate for to the web server host hardware configuration. In the preferred mode of the present invention, web server software 96 is hosted on Windows IIS- based server available from Microsoft Corporation..

Cool ICE system software 98 consists of Cool ICE Object (the gateway) 100, Cool ICE service handler 102, Cool ICE administration 104, Cool ICE repository 106, and Cool ICE Scripting Engine 108. It is these five software modules which establish and maintain an interface to web server software 96 using COM interfaces and interface to Cool ICE's internal and external data base management systems.

Cool ICE object 100 is the interface between standard, commercially available, web server software 96 and the internal Cool ICE system scripting engine with its language and logic facility. As such, Cool ICE object 100 translates the dialog format, incoming HTML service request into internal Cool ICE requests for service. Intrinsic in this translation is a determination of the service category (see also Fig. 4) -- that is whether the service request is a native service (i.e., with a default Cool ICE server-side scripting) or an open service (i.e., with server-side scripting in

another commercial language using the Cool ICEA object 100).

The service request, received from Cool ICE object 100, is utilized by Cool ICE service handler 102 to request the corresponding service action script from Cool ICE repository 106 and to open temporary state storage using Cool ICE repository 106. Cool ICE service handler 102 sequences through the service input variables of the object received from Cool ICE object 100 and transfers each to Cool ICE repository 106 for temporary storage until completion of the service request. Cool ICE service handler 102 retrieves the intermediate products from Cool ICE repository 106 upon completion of the service request and formulates the Cool ICE response for transfer to browser 92 via web server software 96 and world wide web path 94.

Cool ICE administration 104 implements automatic and manual control of the process. It provides for record keeping, for resolution of certain security issues, and for development of further Cool ICE objects. Interconnect 110 and interconnect 112 are software interface modules for communicating over the enterprise network (see also Fig. 4). These modules are dependent upon the remaining proprietary hardware and software elements coupled to the enterprise network system. In the preferred mode of the present invention, these are commercially available from Unisys Corporation.

Fig. 6 is a schematic diagram 116 showing the processing of a service request by the Cool ICE system. Screen 118 is the view as seen by the client or user at an internet terminal (see also Fig,. 4). This screen is produced by the commercially available browser 120 selected by the user. Any such industry standard browser is suitable, if it has the capability to handle frames. The language of screen 118 is HTML 124. Hyperlinks 126 is used in locating the URL of the Cool ICE resident server. The components of the URL are as follows. In many instances, this will simply be the internet access provider of the internet terminal, as when the internet terminal is owned by the enterprise and the user is an employee. However, when the user is not an employee and the internet terminal is not necessarily owned by the enterprise, it becomes more likely that hyperlinks 126 identifies a remotely located server.

Icon 122 is a means of expressly identifying a particular service request. Such use of an icon is deemed to be unique. Additional detail concerning this use of an icon is available in the above identified, commonly assigned, co-pending U.S. Patent application. Window area 128 provides for the entry of any necessary or helpful input parameters. Not shown are possible prompts for entry of this data, which may be defined at the time of service request development. Submit button provides the user with a convenient means to transmit the service request to the web server in which the Cool ICE system is resident.

Upon "clicking on" submit button 130, screen 118 is transmitted to web server 136 via world wide web path 132. As discussed above, world wide web path 132 may be a telephonic dial-up of web server 136 or it might be a long and complex path along the internet if web server 136 is remote from the originating internet terminal. Web server 136 is the software which

performs the retrieval of screen 118 from world wide web path 132.

Screen 118 is transferred from web server 136 to Cool ICE object 138, wherein it is converted to the internal Cool ICE protocol and language. A browser input is opened at storage resource 166 via path 150 and path 151. Thus the initial service request can be accessed from storage resource 166 during processing up until the final result is transferred back to the user. This access readily permits multi-step and iterative service request processing, even though the service request was transferred as a single internet dialog element. This storage technique also provides initially received input parameters to later steps in the processing of the service request.

Cool ICE object 138 notifies Cool ICE service handler 156 through the Cool ICE Engine Interface 157 that a service request has been received and logged in. The service request itself is utilized by Cool ICE service handler 156 to retrieve a previously stored sequence of data base management system command statements from repository 166. Thus, in the general case, a single service request will result in the execution of a number of ordered data base management system commands. The exact sequence of these commands is defined by the service request developer as explained in more detail below.

Service input parameters 170 is prepared from the service request itself and from the command sequence stored in repository 166 as shown by paths 164 and 165. This list of input parameters is actually stored in a dedicated portion of repository 166 awaiting processing of the service request.

Each command statement from repository 166 identified with the service request object is sequentially presented to a Cool ICE service 168 for processing via path 160. The corresponding input parameters 170 is coupled with each command statement via path 176 to produce an

appropriate action of the enterprise data base management system at Cool ICE service 168. After the enterprise data base management system has responded to a given query, the intermediate products are stored as entries in HTML document 172 which is also stored in a dedicated portion of repository 166.

After all command statements corresponding to the service request have been processed by the enterprise data base management system and HTML document 172 has been completed, the result is provided via path 158 to Cool ICE Engine Interface 157. Cool ICE object 138 receives the browser output via path 150. The response is converted to HTML protocol and transferred by web server 136 and world wide web path 134 to be presented to the user as a modified screen (not shown).

Fig. 7 is a pictographic drawing 178 of the development process for creating a Cool ICE service. HTML document 180 is created utilizing any commercially available standard HTML authoring tool (e.g., Microsoft FrontPage). The resulting HTML document 180 is stored as a normal .HTM file. This file will be utilized as a template of the service to be developed.

The authoring process moves along path 182 to invoke the administration module of the Cool ICE system at element 184. The new dynamic service is created using HTML document 180 stored as a normal .HTM file as a template. As HTML document 180 is imported into Cool ICE, sequences of script for the beginning and end of the HTML code are automatically appended to the service. Required images, if any, are also uploaded onto the web server (see also Figs. 5 and 6). The service is edited by inserting additional Cool ICE script, as required. A more detailed description of the editing process may be found in Cool ICE User's Guide, Revision 2.0, available from Unisys Corporation and incorporated herein by reference.

The completed service script is transferred along path 186 to element 188 for storage. The service is stored as a service object in the repository (see also Figs. 5 and 6). Storage is effected within the appropriate category 190 as discussed above, along with services 192, 194, and 196 within the same category.

The process proceeds along path 198 to element 200 for testing. To perform the testing, the URL for the newly created service is entered into the browser of the internet terminal, if known. The typical URL is as follows:

http://machine-name/CoolICE/default.asp?Category=Examples&Service=FRMEX01

If the URL for the new service is not known, a list of the available services may be determined

from the Cool ICE system by specifying the Cool ICE URL as follows:

http;://machine-name/Cool-ICE

This call will result in a presentation of a menu containing the defined categories. Selecting a category from the list will result in a menu for the services defined within that category. The desired service can thus be selected for testing. Selection of the service by either means will result in presentation of the HTML page as shown at element 200.

The process proceeds to element 204 via path 202, wherein the HTML page may be enhanced. This is accomplished by exporting the HTML document from the Cool ICE administration module to a directory for modification. By proceeding back to HTML document 180 via path 208, the exported HTML template is available for modification using a standard HTML authoring tool. After satisfactory completion, the finished HTML document is saved for future use.

Fig. 8 is a diagram showing a comparison between dialog-based structure 210 and service-based structure 212. Dialog-based structure 210 is the norm for the typical existing proprietary data base management system (e.g., MAPPER). The user, normally sitting at a dedicated user terminal, transfers output screen 214 to the data base management system to request a service. The user terminal and its normally dedicated link are suspended at element 216 to permit transfer and operation of the data base management system. The input is validated at element 218, while the user terminal and its normally dedicated link remains suspended.

The data base management system processes the service request at element 220 while the user terminal remains suspended. Output occurs at element 222 thereby releasing the suspension of the user terminal. Thus, a true dialog is effected, because one part of the dialog pair (i.e., the user terminal) is suspended awaiting response from the data base management system. This type of dialog is best accomplished in an environment wherein at least the user terminal (or data base management system) is dedicated to the dialog, along with the link between user terminal and data base management system.

Service-based structure 212 illustrates one of the basic constraints of the world wide web protocol. To ensure that each of the elements on the world wide web are sufficiently independent and to prevent one element from unduly delaying or "hanging-up" another element to which it is coupled awaiting a response, the communication protocol forces a termination after each transmission. As can be readily seen, even the simplest dialog requires at least separate and independent transactions or services. The first service, Service 224, involves the transmissions of output form 228 from the internet user terminal. This transmission is immediately and

automatically followed by termination 230 to ensure independence of the sender and receiver.

The second service, Service 226, enables the receiver of output form 228 to process the request and output an appropriate response. The validation of the input at element 232, processing 234, and output 236 all occur within the receiver of output form 228. Immediately and automatically, termination 238 follows. Thus, if internet transactions are to be linked into a true dialog to permit data base management functions, the state must be saved from one service to the next as taught herein.

In the preferred mode of the present invention, the state of a service is saved in the repository (see also Figs. 4 and 5) for use in the next or subsequent services.

Fig. 9 is a schematic diagram 240 of the preferred mode of the present invention showing normal data flow during operation, with special attention to the state saving feature. Work station 242 is an industry compatible personal computer operating under a commonly available operating system. Browser 244 is a standard, commercially available web browser having frames capability. Path 248 is the normal world wide web path between work station 242 and web server 254 for the transfer of service requests and input data. These transfers are converted by Cool ICE object 256 as explained above and sent to Cool ICE Engine Interface 259 for disposition.,

The service request for data and/or another function is converted into the data base management language by reference to the service definition portion of repository 262 through reference along path 276. The actual command language of the data base management system is utilized over path 286 to access data base 264. The resultant data from data base 264 is transferred to Cool ICE object 256 via path 288. State manager 260 determines whether the original service request requires additional queries to data base 264 for completion of the dialog. If yes, the resultant data just received from data base 264 is transferred via path 284 to repository 262 for temporary storage, and the next query is initiated over path 286, and the process is repeated. This is the state saving pathway which is required to provide the user of the Cool ICE system to function in a dialog mode over the world wide web.

Upon receipt of the resultant data from the final query of data base 264, state manager 260 determines that the service request is now complete. State manager 260 notifies repository 262 via path 280, and the intermediate products are retrieved from temporary storage in repository 262 via path 278 and supplied to Cool ICE service handler 258 via path 272 for

formatting. State manager 260 then clears the intermediate products from temporary storage in repository 262 via path 282. The final response to the service request is sent to Cool ICE object 256 via path 270 for manipulation, if necessary, and to browser 244 via path 250.

Fig. 10 is a detailed diagram 300 showing operation of the security system during the honoring of a service request. The user, operating industry compatible, personalized computer, workstation 302, formats a service requests via commercially available web browser 304. In the preferred mode of the present invention, this is accomplished by then making a call to the Cool ICE system. The user simply requests access to the Cool ICE home page by transferring web browser 304 to the URL of Cool ICE system. After the Cool ICE home page has been accessed, one of the buttons is clicked requesting a previously defined service request. For additional detail on the service request development process, see above and the above referenced commonly assigned, co-pending U.S. Patent Applications.

The service request is transferred to web server 314 via world wide web path 306. The service request is received by Cool ICE object 322 and translated for use within the Cool ICE system. The request is referred to the Cool ICE Engine Interface 331 via path 324. In the preferred mode of practicing the present invention, the Cool ICE Engine Interface 331 is equivalent to the MAPPER data base management system. The service request is passed to Cool ICE Service Handler 332 for retrieval of the command language script which describes the activities required of the data base management system to respond to the service request.

Cool ICE Service Handler 332 makes an access request of Cool ICE service portion 340 of repository 342 via path 338. It is within Cool ICE service portion 340 of repository 342 that the command language script corresponding to the service request is stored. The command language script is obtained and transferred via path 336 to service handler 332 for execution. Along with the command language script, a security profile, if any, is stored for the service

request. As explained in the above referenced, commonly assigned, co-pending U.S. Patent Application, the security profile, if required, is added to the command language script file at the time of service request development by the service request developer. This security profile identifies which of the potential service requestors may actually be provided with a complete response. The security profile, if any, is similarly transferred to service handler 332 via path 336.

If no security profile has been identified for the service request, service handler 332 allows the execution of the command language script received via path 336 through access of remote database 316 via paths 318 and 320, as required. The response is transferred to Cool ICE object 322 via path 328 for conversion and transfer to workstation 302 via world wide web path 310.

However, if a security profile has been identified for the service request, service handler 322 requests the user to provide a user-id via path 330, Cool ICE object 322, and world wide web path 312. Service handler 332 awaits a response via world wide web path 308, Cool ICE object 322, and path 326. Service handler 332 compares the user-id received to the security profile stored with the command language script. If the user matches the security profile, access is granted and service handler 322 proceeds as described above. If the user does not match with the stored security profile, the service request is not executed and the user is notified via an appropriate message.

Fig. 11 is a view of the highest level window 344 of Cool ICE Administration (see also above). It is the Cool ICE Administration module which is responsible for maintaining the security profiles of each service request and data element. Cool ICE Administration window 344, as identified by title 346, is displayed in response to a request issued by an accompanying windows program called MAPPER Presentation Client, MPC, (not shown). Security button 348 is provided for access to the security maintenance functions of the Cool ICE Administration module. Clicking on security button 348 provides entry to the security maintenance functions.

Fig. 12 is a view of security maintenance main window 360, which is reached by clicking on security button 348 (see also above). Of course, access to security maintenance main window 360 requires a user-id correlating with a security profile adequate to security profile maintenance. Title 362 identifies security maintenance main window 360.

The user must access the security profile table of the service request and/or data base of interest using select button 378. In the present example, the manager from the human resources department is utilizing internet terminal 378 to maintain the view of the security definitions for data base 352 (see also Fig. 11). The interface hierarchy provides a list 386 of the tables within data base 352. Authority caption 388 is selected providing access to the security profiles for Authority 356 (see also Fig. 11).

The security profiles currently corresponding to Authority 356 are displayed in the profile window. HR 380 shows that the human resources security profile is to be provided access to table Authority 356 of data base 352. Similarly, A. Payable 382 shows that the accounts payable manager previously identified as the user of internet terminal 382 is also to be provided access to Authority 356 of data base 352. Empty space 384 shows that no other security profiles are currently to be provided access to Authority 356.

Button 368 enables an authorized user to add an additional security profile for access to Authority 356. Button 370 permits and authorized user to modify an existing security profile. Button 372 permits removal of a security profile. Button 374 establishes reinheritance. Button 376 provides an authorized user with a report of the security profiles corresponding to a given data table. Button 366 permits the user to save a new or modified security profile allocation. The

remaining buttons are deemed to be self explanatory.

Fig. 13 is a class diagram showing creation of a site security profile.

Fig. 14 is a listing of the messages associated with creation of a site security profile.

Having thus described the preferred embodiments of the present invention, those of skill in the art will be readily able to adapt the teachings found herein to yet other embodiments within the scope of the claims hereto attached.

WE CLAIM:

CLAIMS

1. In a data processing environment having a user terminal at a site for generating a service request responsively coupled via a publically accessible digital data communication network to a data base management system having at least one data base, the improvement comprising:

a security profile corresponding to said site whereby said data base management system permits said user terminal to access said at least one data base.

2. The improvement according to claim 1 wherein said security profile is generated by said data base management system.

3. The improvement according to claim 2 further comprising a special field responsively coupled to said service request whereby said data base management system receives said special field and generates said security profile corresponding to said site.

4. The improvement according to claim 3 wherein said publically accessible digital data communication network further comprises the internet.

5. The improvement according to claim 4 wherein said data base management system is MAPPER.

6. An apparatus comprising:

a. a user terminal located at a site;

b. a data base management system having access to a data base responsively coupled to said user terminal via a publically accessible digital data communication network; and

c. a security profile generated by said data base management system corresponding to said site whereby said data base management system provides access to a particular portion of said data base corresponding to said security profile.

7. The apparatus of claim 6 wherein said user terminal accesses said data base by transferring a service request to said data base management system.

8. The apparatus of claim 7 wherein said service request further comprises a special field corresponding to said site.

9. The apparatus of claim 8 wherein said data base management system further comprises MAPPER.

10. The apparatus of claim 9 wherein said publically accessible digital data communication network further comprises the world wide web.

11. A method of utilizing a user terminal located at a site to access a remote data base management system having a data base via a publically accessible digital data communication

network comprising:

a. transmitting a service request requiring access to said data base from said user terminal;

b. receiving said service request by said remote data base management system;

c. determining a security profile corresponding to said site;

d. comparing said security profile with said service request; and

e. honoring said service request if and only if said service request corresponds to said security profile

12. A method according to claim 11 wherein said transmitting step further comprises transmitting a special field.

13. A method according to claim 12 wherein said determining step further comprises generating said security profile corresponding to said special field.

14. A method according to claim 13 wherein said publically accessible digital data communication network further comprises the internet.

15. A method according to claim 14 wherein said remote data base management system further comprises the MAPPER data base management system.

16. An apparatus comprising:

a. means located at a site for permitting a user to interact with a data base responsively coupled via a publically accessible digital data communication network;

b. means responsively coupled to said permitting means via said publically accessible digital data communication network for offering data processing services involving access to said data baser in response to said service request;

c. means responsively coupled to said offering means for preventing said offering means from offering said data processing services to said user in response to said service request unless said site corresponds to a security profile wherein said security profile permits access to said data base.

17. An apparatus according to claim 16 wherein said publically accessible digital data communication network further comprises the internet.

18. An apparatus according to claim 17 wherein said permitting means further comprises means for transmitting a special field corresponding to said site.

19. An apparatus according to claim 18 wherein said offering means further comprises MAPPER data base management system.

20. An apparatus according to claim 19 wherein said permitting means further comprises an industry standard personal computer.

ABSTRACT OF THE DISCLOSURE

An apparatus for and method of utilizing an internet terminal coupled to the world wide web to access an existing proprietary data base management system having a dialog-based request format. The user request is received by a web server from the world wide web and converted into one or more sequenced data base management commands stored as corresponding to the service request. If a particular service request requires access to secured data and/or services, the request may be granted in relationship to a particular user security profile. This security profile is determined through a special field indicative of the internet user transferred in conjunction with the service request.

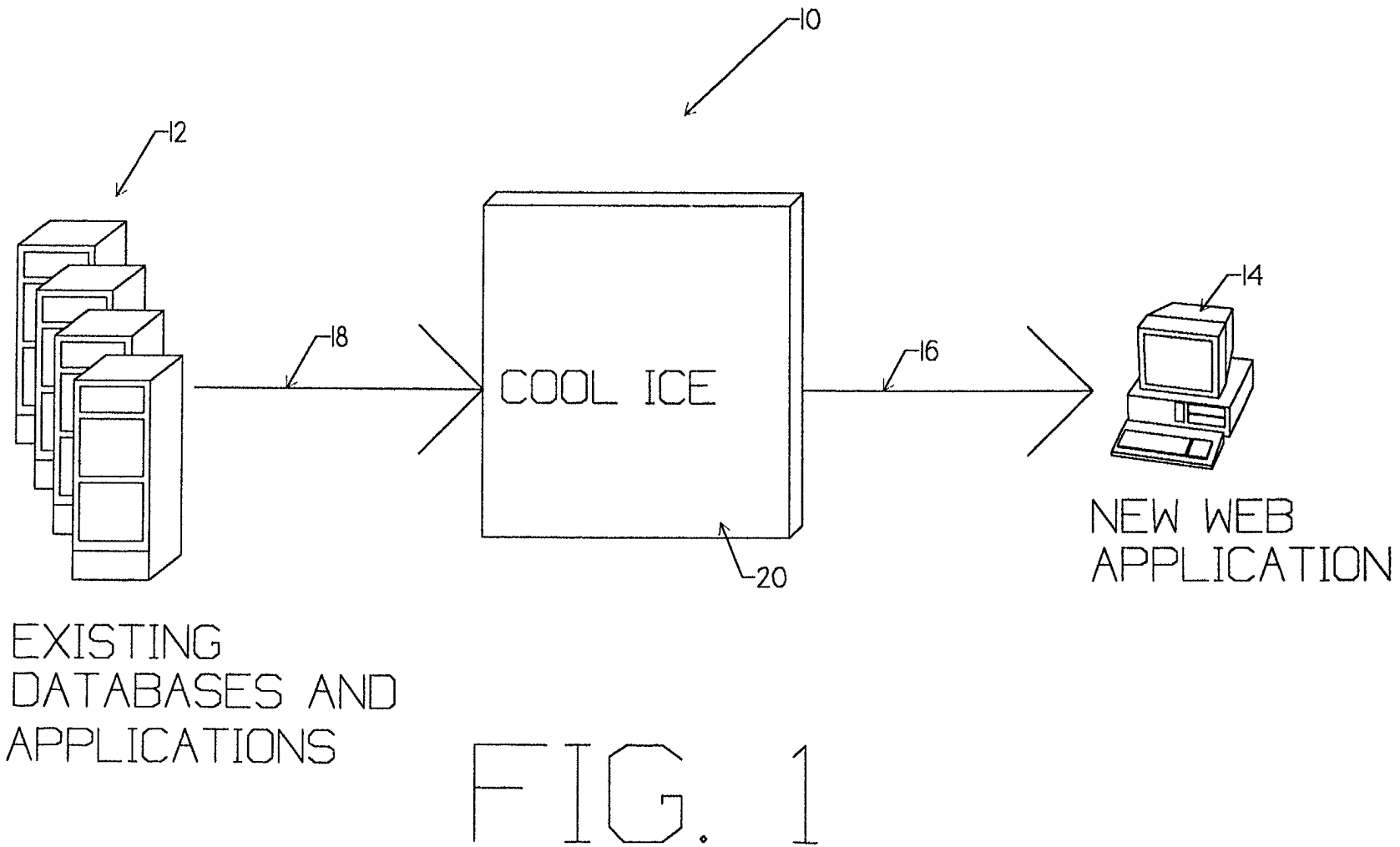
10
12
18
COOL ICE
16
14
20
NEW WEB
APPLICATION
EXISTING
DATABASES AND
APPLICATIONS

FIG. 1

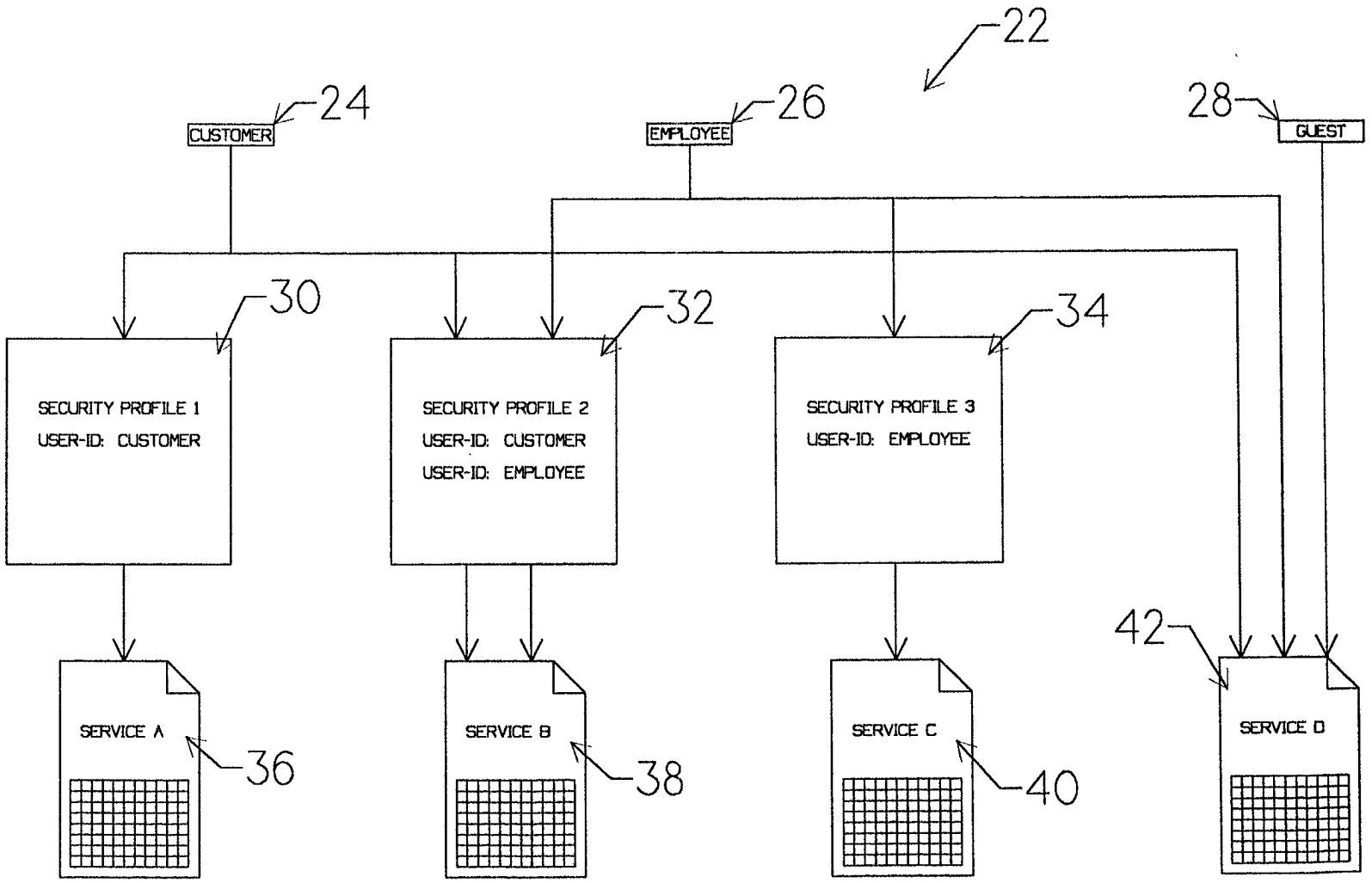
22
24
CUSTOMER
26
EMPLOYEE
28
GUEST
30
32
34
SECURITY PROFILE 1
USER-ID: CUSTOMER
SECURITY PROFILE 2
USER-ID: CUSTOMER
USER-ID: EMPLOYEE
SECURITY PROFILE 3
USER-ID: EMPLOYEE
42
SERVICE A
36
SERVICE B
38
SERVICE C
40
SERVICE D

FIG. 2

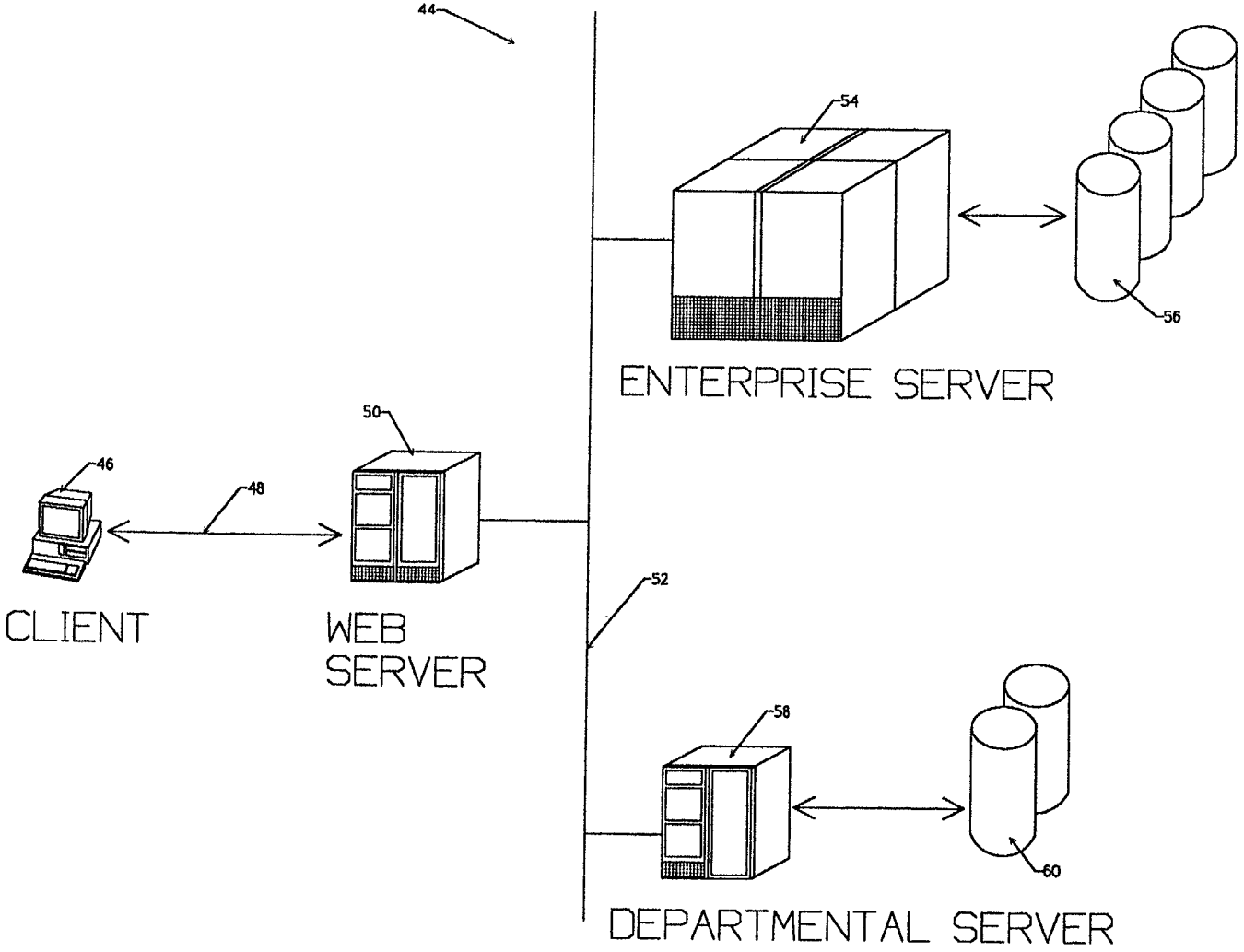
44
54
56
ENTERPRISE SERVER
50
46
48
CLIENT
WEB
SERVER
52
58
60
DEPARTMENTAL SERVER

FIG. 3

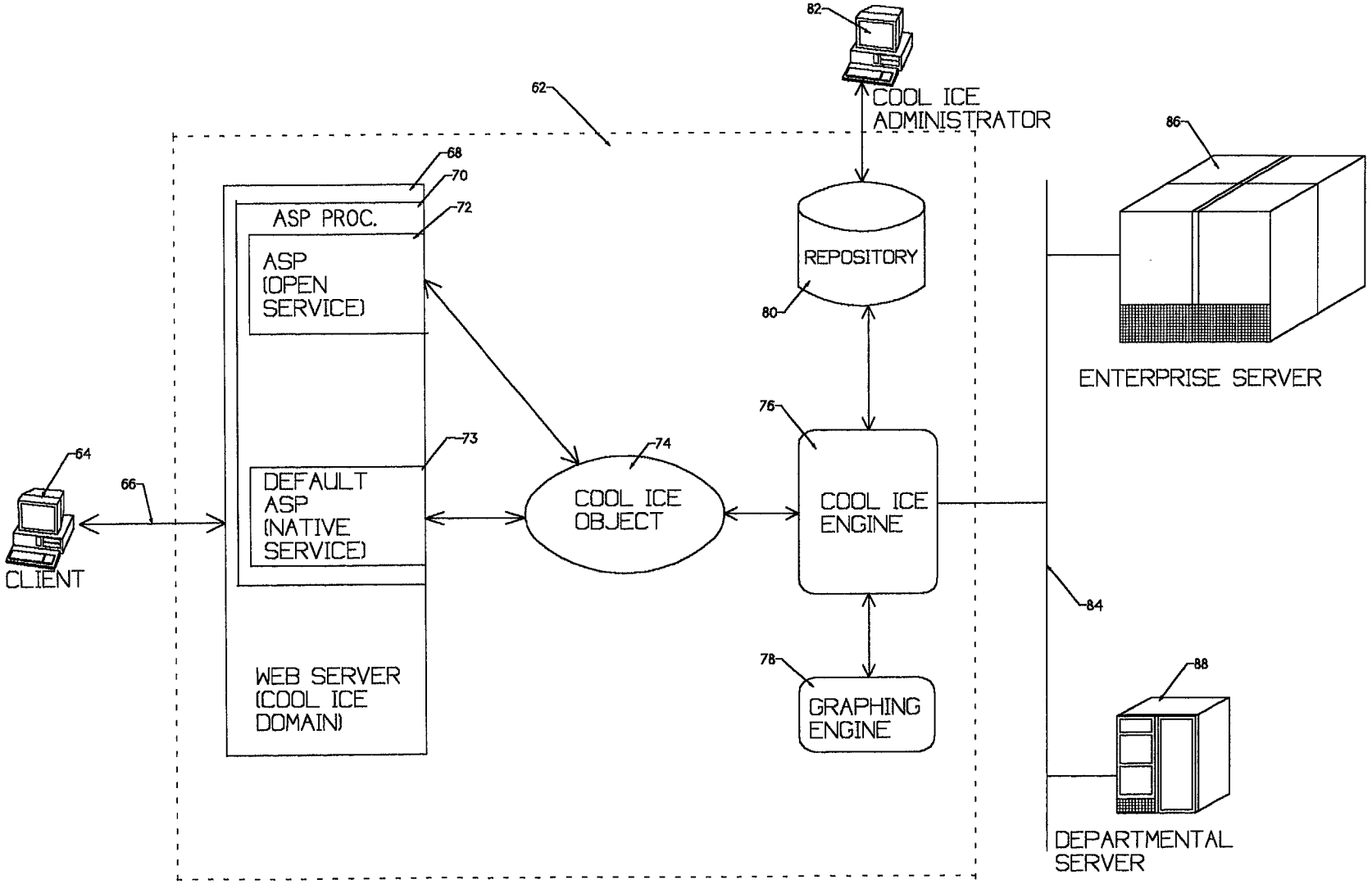
82
COOL ICE ADMINISTRATOR
62
68
70
72
ASP PROC.
ASP (OPEN SERVICE)
DEFAULT ASP (NATIVE SERVICE)
73
WEB SERVER (COOL ICE DOMAIN)
REPOSITORY
80
86
ENTERPRISE SERVER
64
66
CLIENT
74
COOL ICE OBJECT
76
COOL ICE ENGINE
84
78
GRAPHING ENGINE
88
DEPARTMENTAL SERVER

FIG. 4

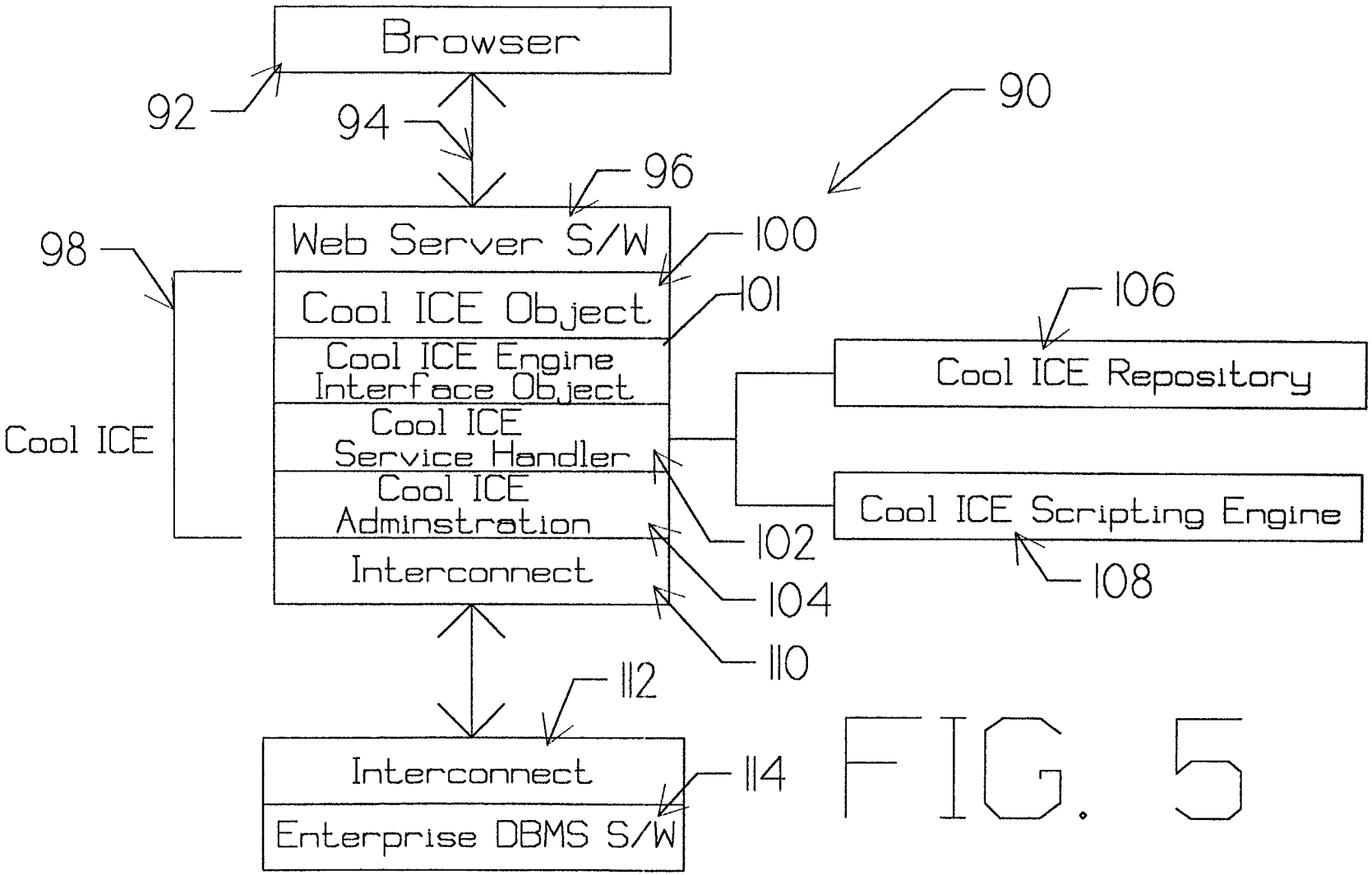
Browser
92
94
90
96
Web Server S/W
100
98
Cool ICE Object
101
106
Cool ICE Engine Interface Object
Cool ICE Repository
Cool ICE
Cool ICE Service Handler
Cool ICE Adminstration
Cool ICE Scripting Engine
102
108
Interconnect
104
110
112
Interconnect
114
Enterprise DBMS S/W

FIG. 5

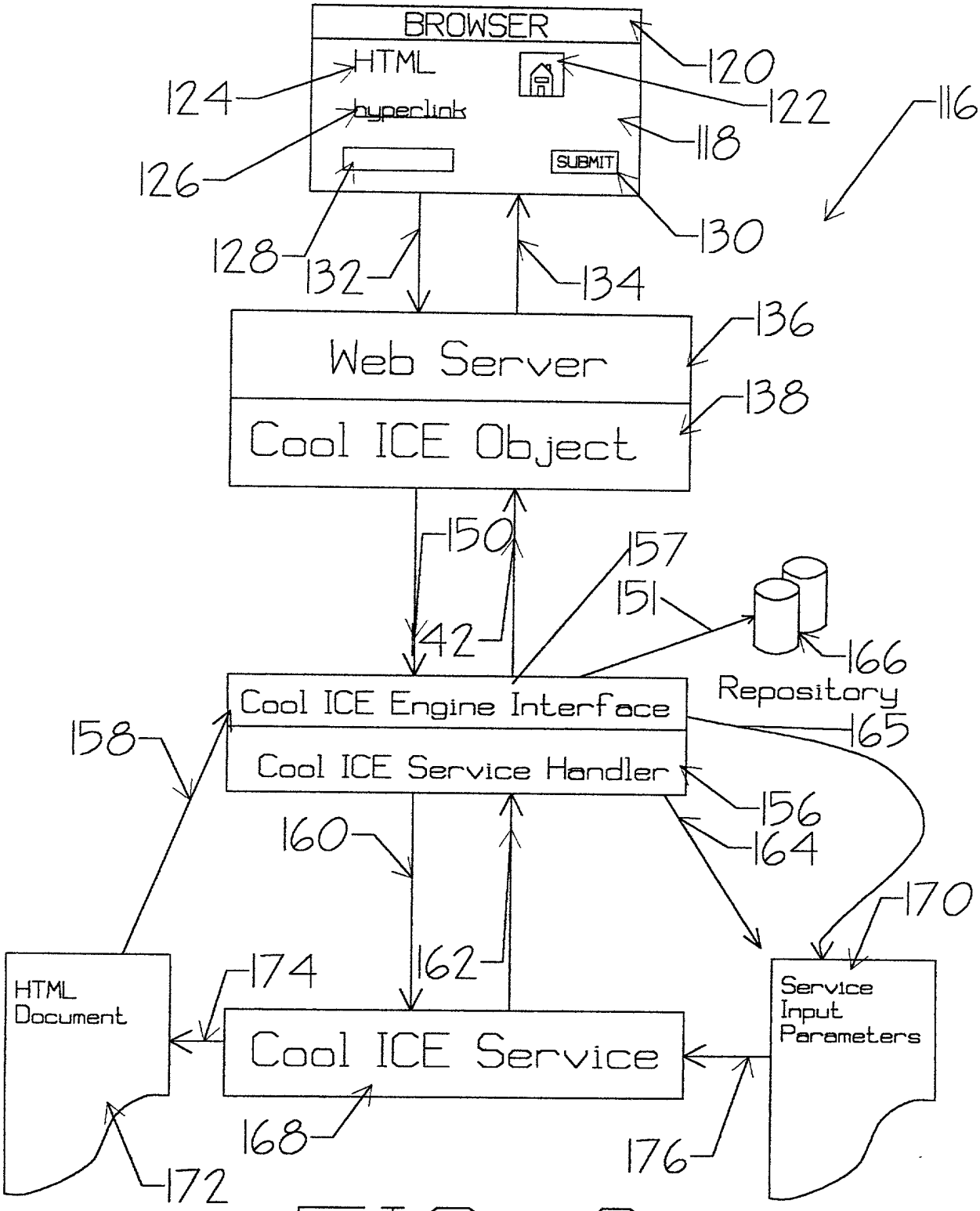
BROWSER
HTML
hyperlink
SUBMIT
120
122
124
126
116
118
128
130
132
134
Web Server
136
Cool ICE Object
138
150
157
151
42
166
Repository
Cool ICE Engine Interface
158
165
Cool ICE Service Handler
156
160
164
170
162
HTML
Document
174
Service
Input
Parameters
Cool ICE Service
168
176
172

FIG. 6

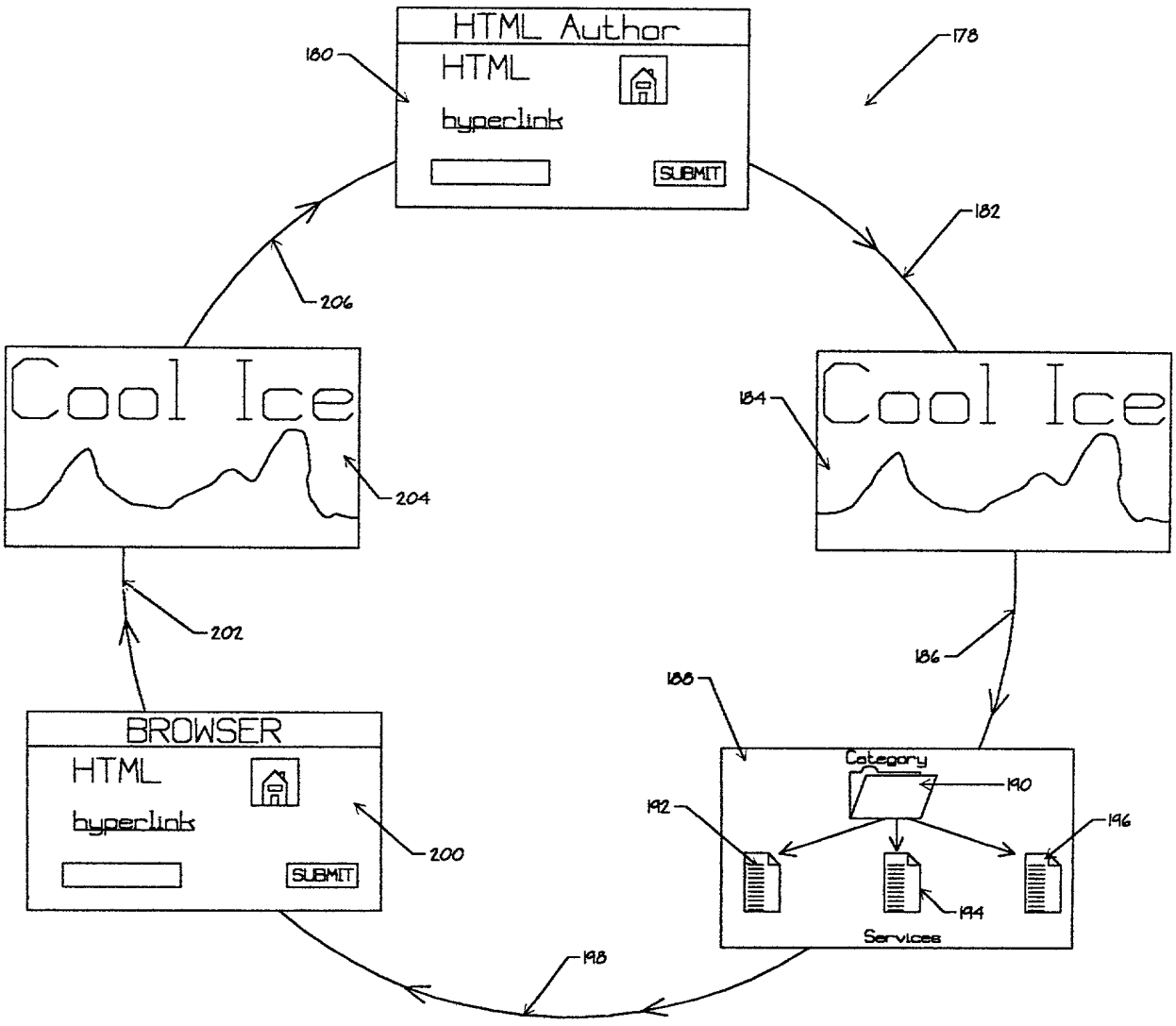
HTML Author
HTML
hyperlink
SUBMIT
178
180
182
206
Cool Ice
204
Cool Ice
184
202
186
188
BROWSER
HTML
hyperlink
SUBMIT
200
Category
190
192
196
194
Services
198

FIG. 7

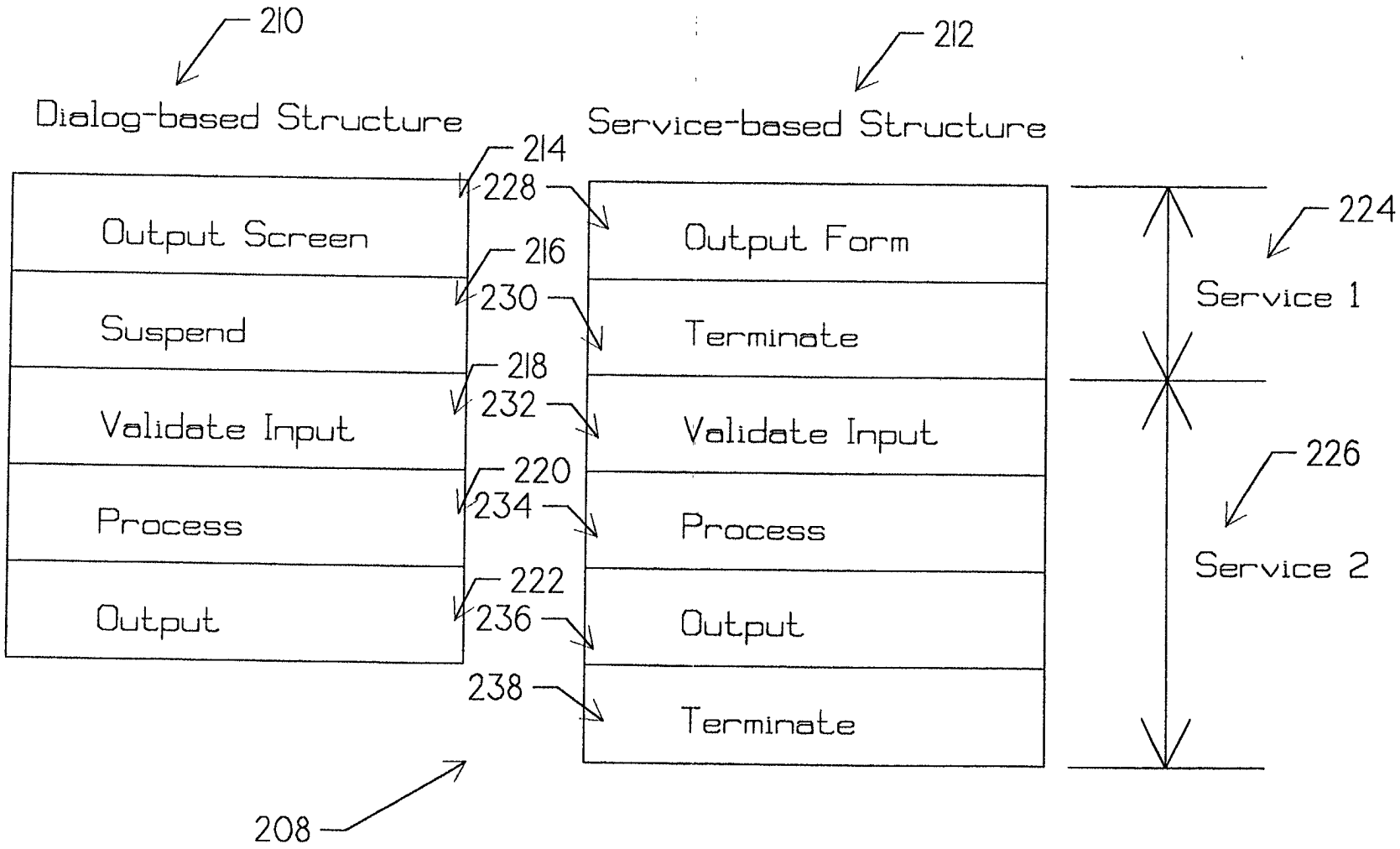
210
Dialog-based Structure
212
Service-based Structure
214
228
216
230
218
232
220
234
222
236
238
Output Screen
Suspend
Validate Input
Process
Output
Output Form
Terminate
Validate Input
Process
Output
Terminate
224
Service 1
226
Service 2
208

FIG. 8

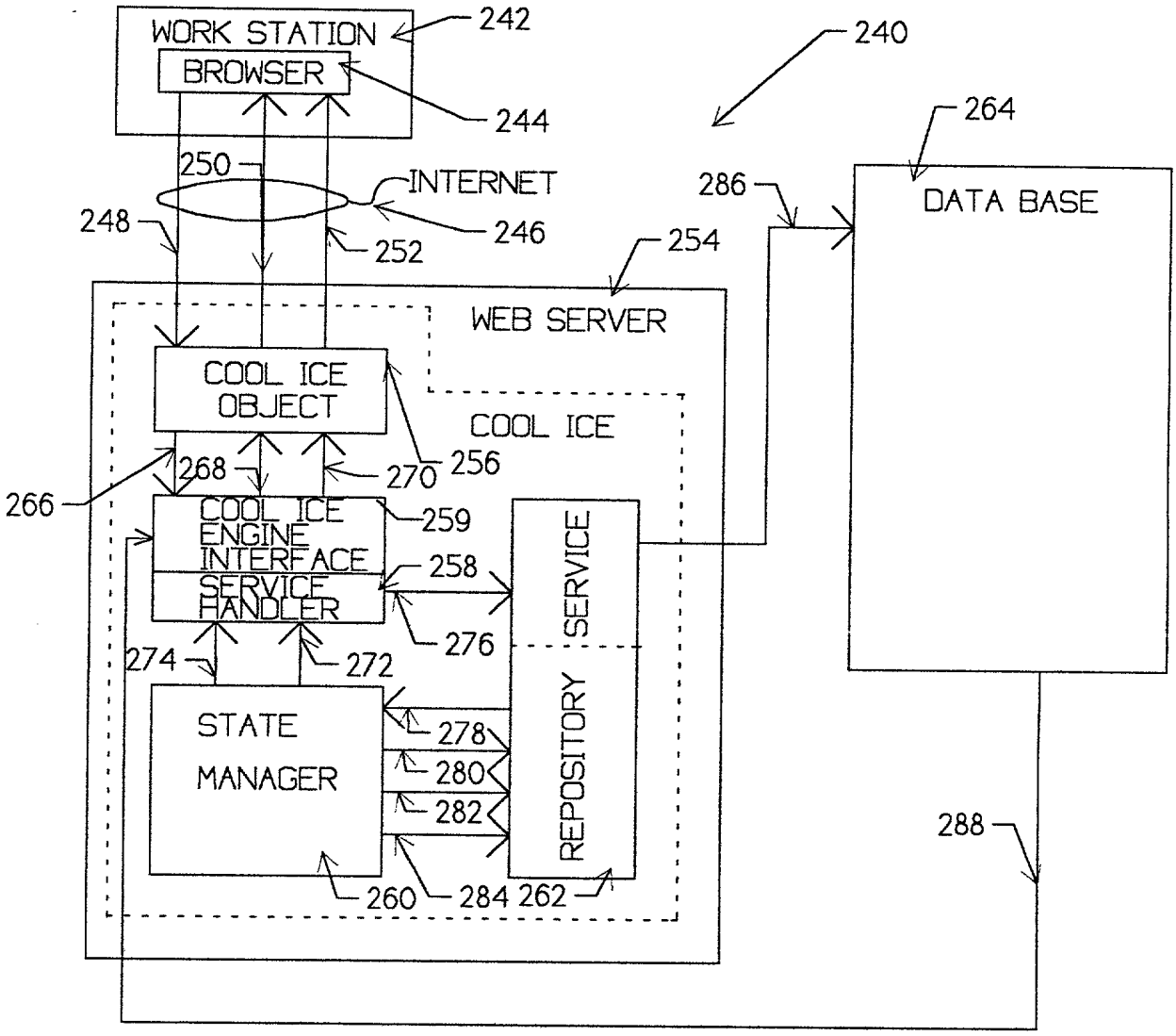
WORK STATION
BROWSER
242
244
240
264
250
INTERNET
286
DATA BASE
248
246
252
254
WEB SERVER
COOL ICE OBJECT
COOL ICE
268
270
256
266
COOL ICE ENGINE INTERFACE
259
SERVICE HANDLER
258
SERVICE
276
274
272
STATE MANAGER
278
280
282
REPOSITORY
288
260
284
262

FIG. 9

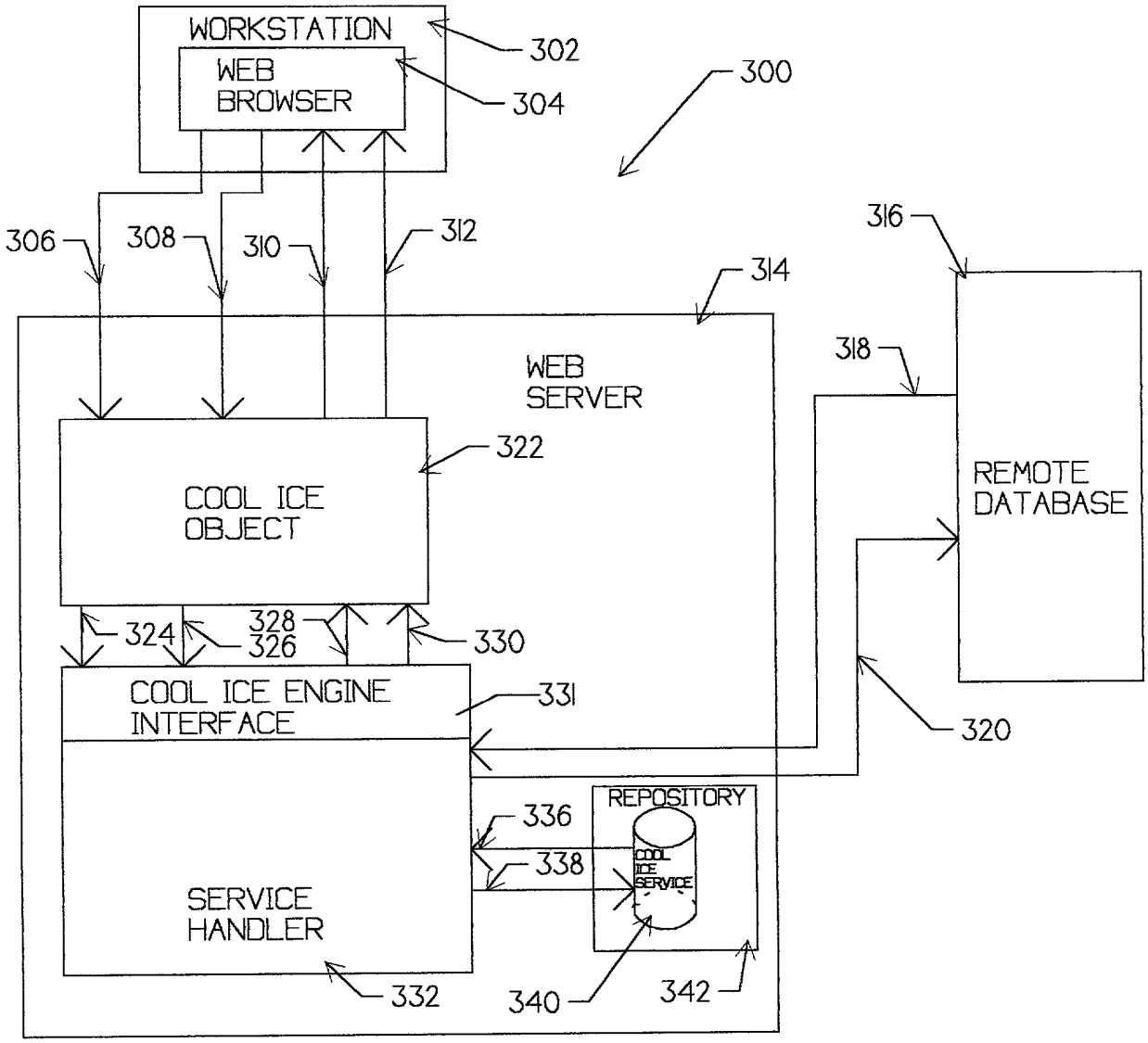
WORKSTATION
WEB BROWSER
302
304
300
306
308
310
312
314
316
318
WEB SERVER
COOL ICE OBJECT
322
REMOTE DATABASE
324
326
328
330
COOL ICE ENGINE INTERFACE
331
320
REPOSITORY
336
338
COOL ICE SERVICE
SERVICE HANDLER
332
340
342

FIG. 10

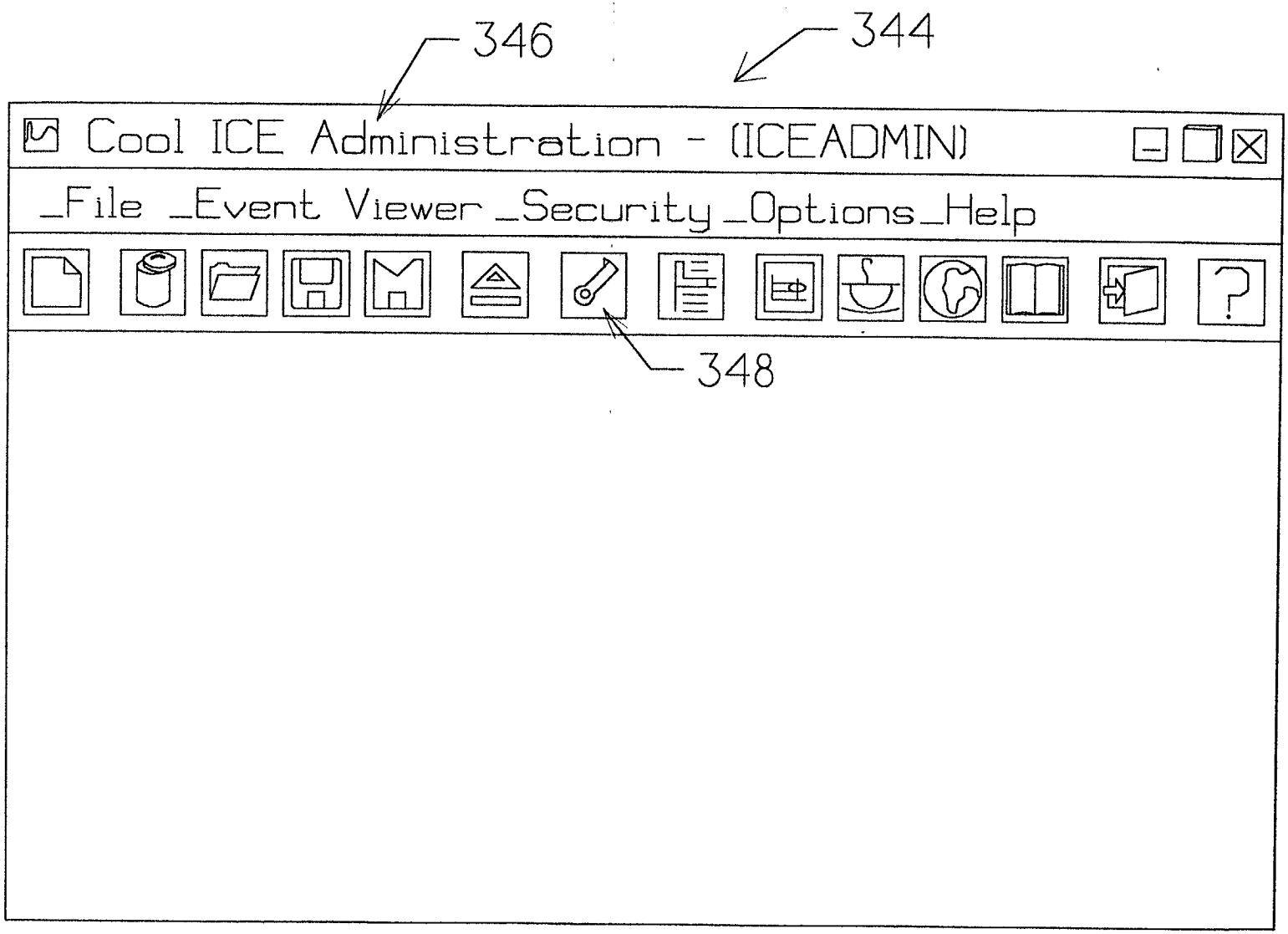
346
344
Cool ICE Administration - (ICEADMIN)
_File _Event Viewer _Security _Options _Help
348

FIG. 11

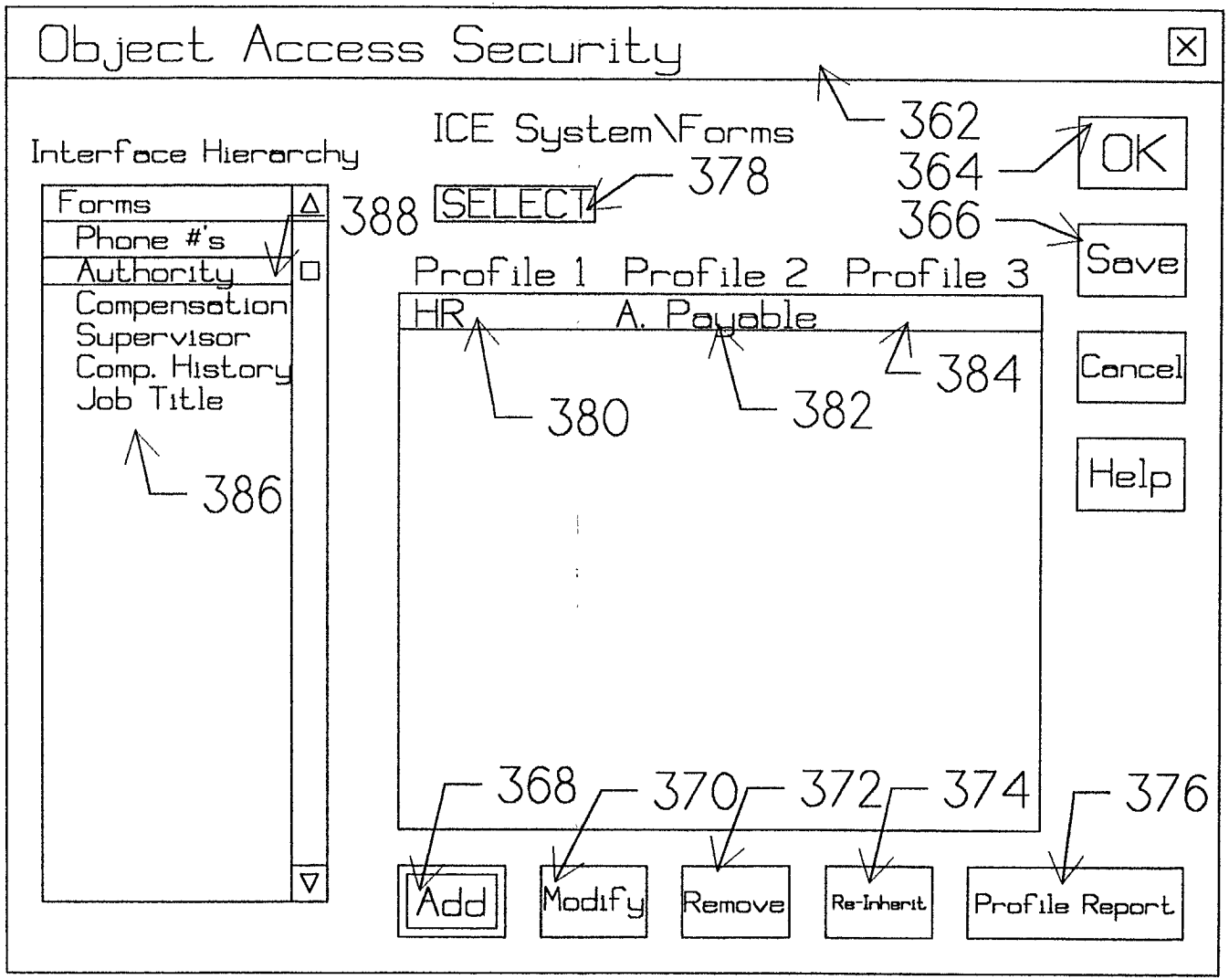
Object Access Security
ICE System\Forms
362
Interface Hierarchy
Forms
Phone #'s
Authority
Compensation
Supervisor
Comp. History
Job Title
386
388
SELECT
378
364
OK
366
Save
Profile 1
Profile 2
Profile 3
HR
A. Payable
380
382
384
Cancel
Help
368
370
372
374
376
Add
Modify
Remove
Re-Inherit
Profile Report
360

FIG. 12

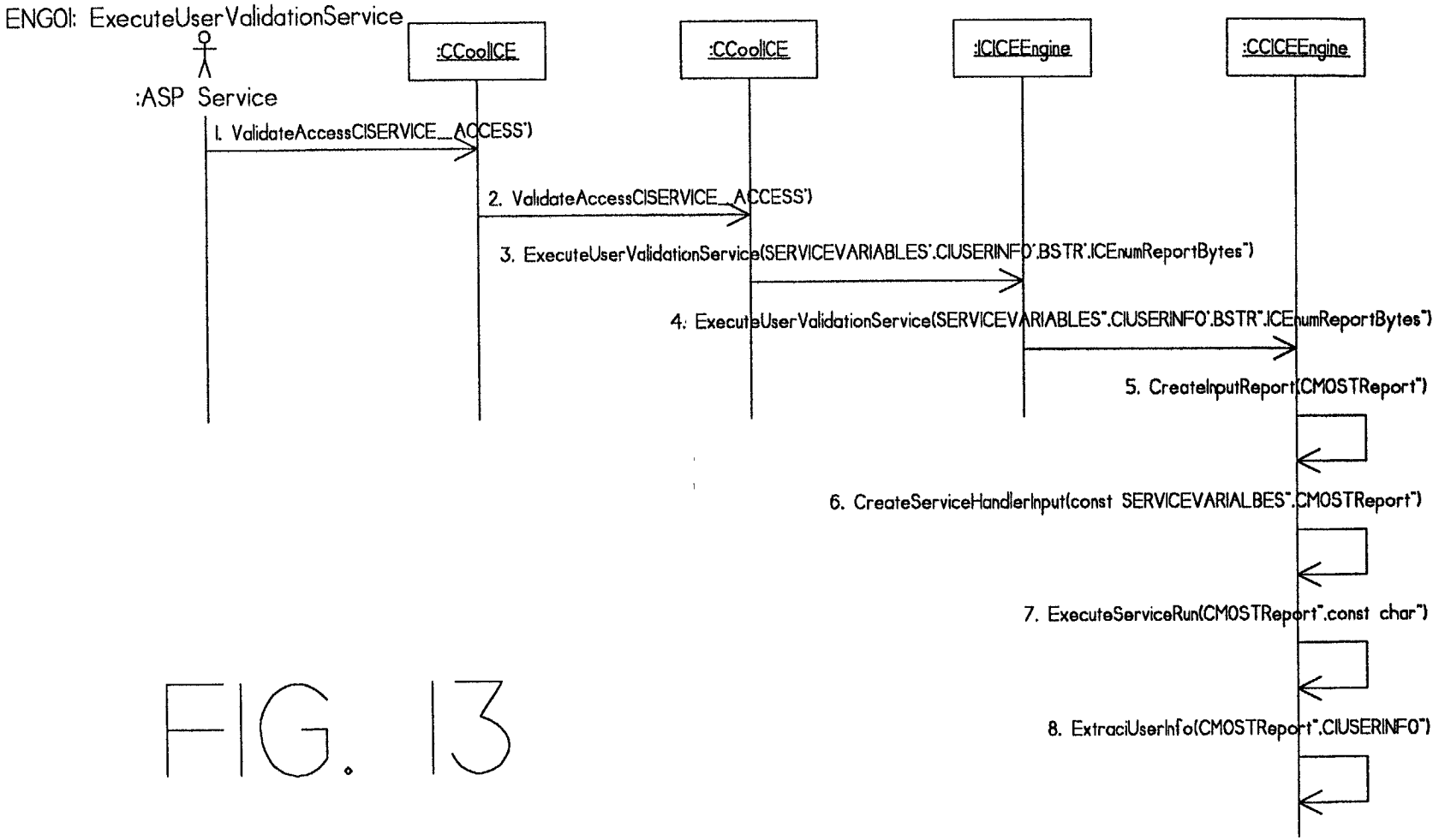
ENG01: ExecuteUserValidationService
:ASP Service
:CCoolICE
:CCoolICE
:ICICEEngine
:CCICEEngine
1. ValidateAccessCISERVICE_ACCESS")
2. ValidateAccessCISERVICE_ACCESS")
3. ExecuteUserValidationService(SERVICEVARIABLES".CIUSERINFO".BSTR".ICEnumReportBytes")
4. ExecuteUserValidationService(SERVICEVARIABLES".CIUSERINFO".BSTR".ICEnumReportBytes")
5. CreateInputReport(CMOSTReport")
6. CreateServiceHandlerInput(const SERVICEVARIALBES".CMOSTReport")
7. ExecuteServiceRun(CMOSTReport".const char")
8. ExtraciUserInfo(CMOSTReport".CIUSERINFO")

FIG. 13

MESSAGE #	DESCRIPTION
1.	The ASP calls the ValidateAccess method to determine the access privileges of the current user.
2.	The ValidateAccess method determines that a user SignOn is required. and the input from the SignOn form is available. When site specific user validation is used. the SignOn form must contain a hidden field with the name "UserValInputForm". When a form with the field name "UserValInputForm" is found. the ExecuteUserValidationService method is called to convert the site specific validation input to a valid userID/department/password.
3.	Call ExecuteUserValidationService to translate the site specific validation input to a valid userID/department/password. The translated data is returned in a CIUSERINFO structure.
4.	This method is called to execute the site specific User Validation service.
5.	Create the service input report.
6.	Populate the input report with the web server variables and form input fields.
7.	Execute the User validation service.
8.	Extract the userID/department/password from the output report generated by the User Validation service. The data is returned in the CIUSERINFO structure.

FIG. 14

COMBINED DECLARATION/POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD AND APPARATUS FOR A WEB APPLICATION SERVER TO PROVIDE FOR WEB USER VALIDATION, the specification of which (check one)

XX is attached hereto

__ was filed on _____
as U.S. Application
Serial No. _____

__ and was amended on (if
applicable) _____

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefit(s) under Title 35, United States Code §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	YES	NO
(Number)	(Country)	(Day/Month/Year Filed)	YES	NO
(Number)	(Country)	(Day/Month/Year Filed)	YES	NO

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as

defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Serial No.)	(Filing Date)	(Status-patented, pending, abandoned)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

John L. Rooney, Reg. No. 28,898;
Lawrence M. Nawrocki, Reg. No. 29,333;
Wayne A. Sivertson, Reg. No. 25,645;
Richard C. Stempkovski, Jr., Reg. No. P-45,130;
Jeffery L. Cameron, Reg. No. 43,527;
Donald A. Jacobson, Reg. No. 22,308; and
Charles A. Johnson, Reg. No. 20,852

Send correspondence to:

Charles A. Johnson
Unisys Corporation
Law Department
M.S. 4773
2470 Highcrest Road
Roseville, Minnesota 55113

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon, I further declare that I understand the content of this declaration.

Full name of sole or first inventor Paul S. Germscheid
Inventor's Signature _____ Date 11/23/99
Residence 3 Summit Court
North Oaks, Minnesota 55127 Citizenship U.S.A.
Post Office Address 3 Summit Court
North Oaks, Minnesota 55127

Full name of second or joint inventor Eugene J. Gretter
Inventor's Signature Eugene J Gretter Date 11/23/99
Residence 7178 Snow Owl Lane
Lino Lakes, Minnesota 55014-1942 Citizenship U.S.A.
Post Office Address 7178 Snow Owl Lane
Lino Lakes, Minnesota 55014-1942

Full name of third or joint inventor Daryl J. Kress
Inventor's Signature Daryl J Kress Date 11/23/99
Residence 16790 Ingersoll Avenue North
Hugo, Minnesota 55038 Citizenship U.S.A.
Post Office Address 16790 Ingersoll Avenue North
Hugo, Minnesota 55038

Full name of fourth or joint inventor Timothy J. Guhl
Inventor's Signature Timothy J Guhl Date 11/23/99
Residence 2905 - 150th Avenue N.W.
Andover, Minnesota 55304 Citizenship U.S.A.
Post Office Address 2905 - 150th Avenue N.W.
Andover, Minnesota 55304

Full name of fifth or joint inventor Gail L. Behr
Inventor's Signature Gail L Behr Date 11/23/99
Residence 3958 Emerson Avenue North
Minneapolis, Minnesota 55412 Citizenship U.S.A.
Post Office Address 3958 Emerson Avenue North
Minneapolis, Minnesota 55412

1.56 Duty to disclose information material to patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or
(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application:

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.